

# WMD First Response: Requirements, Emerging Technologies, and Policy Implications

*E. S. Vergino and W. E. Hoehn, Jr.*

This article was submitted to  
WMD First Response: Requirements, Emerging Technologies, and  
Policy Implications  
Washington, DC  
September 27-28, 1999

**U.S. Department of Energy**

Lawrence  
Livermore  
National  
Laboratory

**June 19, 2000**

## DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint is made available with the understanding that it will not be cited or reproduced without the permission of the author.

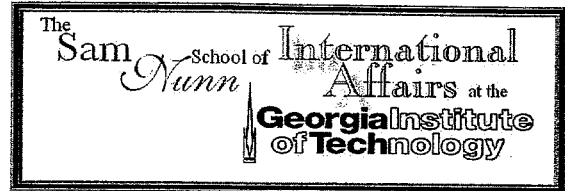
This report has been reproduced  
directly from the best available copy.

Available to DOE and DOE contractors from the  
Office of Scientific and Technical Information  
P.O. Box 62, Oak Ridge, TN 37831  
Prices available from (423) 576-8401  
<http://apollo.osti.gov/bridge/>

Available to the public from the  
National Technical Information Service  
U.S. Department of Commerce  
5285 Port Royal Rd.,  
Springfield, VA 22161  
<http://www.ntis.gov/>

OR

Lawrence Livermore National Laboratory  
Technical Information Department's Digital Library  
<http://www.llnl.gov/tid/Library.html>

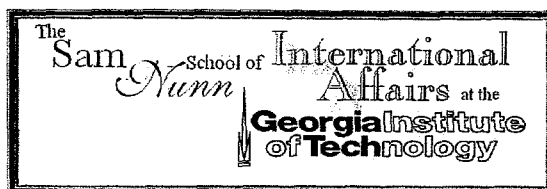


## **WMD FIRST RESPONSE: REQUIREMENTS, EMERGING TECHNOLOGIES, AND POLICY IMPLICATIONS**

by

Eileen S. Vergino and William E. Hoehn, Jr.

This work was performed under the auspices of the U.S. Department of Energy by the University of California, Lawrence Livermore National Laboratory under contract No. W-7405-Eng-48.



## **WMD FIRST RESPONSE: REQUIREMENTS, EMERGING TECHNOLOGIES, AND POLICY IMPLICATIONS**

by  
Eileen S. Vergino<sup>1</sup> and William E. Hoehn, Jr<sup>2</sup>

---

### **Introduction**

In the US today, efforts are underway to defend against the possible terrorist use of weapons of mass destruction (WMD) against US cities. These efforts include the development and adaptation of technologies to support prevention and detection, to defend against a possible attack, and, if these fail, to provide both mitigation responses and attribution for a WMD incident. Technologies under development span a range of systems, from early detection and identification of an agent or explosive, to diagnostic and systems analysis tools; and to forensic analysis for law enforcement. Also, many techniques and tools that have been developed for other applications are being examined to determine whether, with some modification, they could be of use by the emergency preparedness, public health, and law enforcement communities.

However, anecdotal evidence suggests the existence of a serious disconnect between the technology development communities and these user communities. This disconnect arises because funding for technology development is derived primarily from sources (principally federal agencies) distant from the emergency response communities, which are predominantly state, county, or local entities. Moreover, the first responders with whom we have worked candidly admit that their jurisdictions have been given, or have purchased for them, a variety of technological devices, typically without consulting the emergency responders about their utility. In private discussions, emergency responders derisively refer to these as a closet full of useless toys. Technology developers have many new and relevant technologies currently in the development pipeline, but most have not been adequately vetted against the field needs or validated for field use.

The Center for Global Security Research at the Lawrence Livermore National Laboratory<sup>3</sup> and the Sam Nunn School of International Affairs at the Georgia Institute of

---

<sup>1</sup> Eileen Vergino is the Deputy Director in the Center for Global Security Research at the Lawrence Livermore National Laboratory.

<sup>2</sup> William Hoehn is the Coca Cola Foundation Eminent Practitioner at the Sam Nunn School of International Affairs at Georgia Tech.

Technology<sup>4</sup> recently sponsored a two-day workshop to bring together some 50 representatives of the emergency response, technology development, and policy communities. Participating in this workshop were first responders (representing law enforcement, public health, and emergency response personnel from Los Angeles County, Salt Lake City, Atlanta, and London, England), technology developers from US government laboratories and universities, and policymakers from both the executive and legislative branches of the federal government.

The workshop had several objectives. First, we wanted the emergency responders to define the utility of various technologies and tools currently available for first response to a WMD event. Second, we expected the workshop to provide input to the technologists directly from the field users, regarding their special requirements for, and constraints on the use of, new emergency response technologies. Third, we planned to expose the first responders to the types of new technologies under development and allow them the opportunity to ask questions and voice their needs. Finally, we planned to provide recommendations to policymakers for new directions for development and investment of technology.

This was an ambitious workshop. In order to accomplish our objectives, we developed two different scenarios for participants to play, or work through. One scenario involved the planning and execution of a special event in a contained facility (in this case a political convention in a major city). The experience base of the emergency responders was relevant to this scenario, with planning already underway in Los Angeles for the upcoming Democratic National Convention, and in Salt Lake City for the 2002 Olympics (as well as the experience from Atlanta with the 1996 summer Olympics). In addition to the up-front planning and continuous monitoring needed in the opening phase of this scenario, the responders had to address both a primary (diversionary) and a secondary attack.

The second scenario involved an actual terrorist assault, using a biological agent (a virus with a low rate of mortality) producing flu-like symptoms in an attack on two cities. The scenario began as an illness outbreak during flu season, masking the number of illnesses from the attack, leading to a delayed identification of the terrorist incident. Following the positive identification of the outbreak due to the biological agent in the second scenario, terrorists threatened to attack other (unnamed) cities with a much more virulent organism, unless certain demands were met. The scenario focused on planning and preparations in a third large metropolitan area for a possible attack. The initial attacks and the ongoing flu epidemics severely taxed the medical communities in the first two cities, who were the first to detect the illness, as well as creating major headaches for

---

<sup>3</sup> The goal of CGSR is to bring scientists and technologists together with analysts from the policy community to study ways in which technology can enhance international security.

<sup>4</sup> At the Sam Nunn School, we train future leaders in international affairs. The School provides students with an understanding of the interdependent and multicultural world in which they live.

law enforcement communities at the federal, state, and local levels who were trying to preclude additional attacks in other cities.

Workshop participants were divided into two teams to play through each scenario (each of which contained three separate scenario moves and several insertions of new information). Each team was comprised of a mix of first responders, technology developers, and policy personnel. A control group was available to provide answers to questions and access to resources. In addition, each team was directed to develop plans and responses for the areas of Emergency Management, Public Safety, Public Health/Medical, and Law Enforcement. Also, given the omnipresence of the US media, teams had to address public affairs and communications aspects and requirements for each game move. A public affairs specialist participated on the control group and was kept quite busy in helping the teams plan media guidance for public officials (in terms of what and what not to say).

The scenarios were played out in complex and often confusing detail illustrating the real life problems that will be encountered by US authorities in dealing with any future WMD terrorist attack. The scenario plays are summarized below.

## **Convention Scenario (CS)**

### **Background**

This scenario involved the planning and execution of a special event in a contained facility (in this case a political convention in a major city). The first part of the scenario play was devoted to preparation for the upcoming event. Once the convention was underway, a series of events unfolded that would test both the adequacy of these plans and the planners and responders ability to deal with crises.

### **Scenario Play**

The CS working group (playing the role of both advance planners and crisis managers) consisted of medical personnel, first responders from three US jurisdictions and one international jurisdiction, technology developers, and congressional staff involved with allocating funding for these technology development programs.

During the first hour of play the team was charged with setting up security arrangements for the convention. They were provided with basic geographic and demographic information about the city where the political convention was to be held, as well as a schedule of events. They were to plan for the areas of Emergency Management, Public Safety, Public Health/Medical, and Law Enforcement. They were to assume that currently available, off the shelf technology could be incorporated in their plans. The CS group was asked to answer the following questions:

- ¥ What resources do you use and how do you deploy them?
- ¥ What is your timeline for deployment?
- ¥ Is the perimeter secured and if so what is the radius (e.g. one block, one mile)?
- ¥ How is the attendance monitored?
- ¥ What form of ID is required, and who provides and who checks the IDs?
- ¥ Are people free to come and go and who monitors their movement?
- ¥ Who is responsible for crisis management?
- ¥ Who makes decisions?

Discussion during this time period was focused on how local law enforcement, fire, medical, and federal personnel would work together to secure the convention center perimeter.

Early in the scenario play, the team initiated their consequence management planning, including the coordination of local, state, and federal resources, law enforcement, fire, medical, and HAZMAT. They established a structure of unified command, including a joint operations center (JOC), that would be comprised of law enforcement, fire and emergency response, and medical consultants. The team described this planning process

as taking place over many months. Implementation activities range from developing the site plan to sweeping and securing the facility the day before the event. The CS working group believed it would take six months to a year to develop the site plan (including addressing hard targets, venue, and surrounding areas).

Approximately one month prior to the event the law enforcement team would post light forces in the vicinity of the convention center for surveillance and monitoring, as well as for hardening targets. One week prior to the event they would conduct bomb sweeps, check the surrounding areas and traffic points, and on the day of the event there would be forces on site who would monitor all entry into the building. The area to be secured would include up to a 0.5 mile radius; however, most emphasis would be placed on a one block radius. Picture IDs with encoded magnetic information would be required for all people participating in the convention, and all security personnel would be required to have a background check. Security personnel would check credentials and issue identification for all workers, conventioners, and concessionaires.

Once the convention began, the second move in the scenario involved the release of a gas within the convention center during the incumbent President's speech. The release took place in the first few rows of the convention center, very near the podium. All of this activity, of course, is televised live throughout the US. Once the release is announced, the crowds within the center surge toward the exits which is also recorded and broadcast live nationally. Concurrent with this event, an RV truck/trailer with outside propane tanks is abandoned nearby on the freeway.

The CS team was confronted with addressing the emergency response, including the following questions:

- ¥ Who handles the media response?
- ¥ How is health care handled?
- ¥ Who is responsible for triage and is this planned ahead?
- ¥ What, if any, prophylaxis is to be done, and on whom, and how?
- ¥ How is the forensic evidence handled?
- ¥ Who has governance? What do you do with the people?
- ¥ When does the perimeter search take place and who is responsible?

In the normal conduct of an event, the team would employ a process referred to as first among equals; that is, the law enforcement of the local jurisdiction takes precedence. However, once abnormal events began to unfold (beginning with the disruptive gas attack inside the convention building) the team rapidly shifted to a crisis management planning and response mode, and the roles began to evolve.

The CS team immediately began on the spot decontamination of conventioners outside the auditorium, and deployed the HAZMAT team in Class A suits to take swipes and air samples. Unfortunately, with currently available technologies and



techniques these would take up to 48 hours for analysis. While this timetable could be accelerated, to do so would require knowing where and how to send the samples to facilities with newer, faster analysis techniques (such as a government R&D laboratory). This is not a routine effort, as these new facilities would have to be validated and the error rate of the techniques would need to be clearly understood (false positives can be a significant health hazard in addressing the public health concerns as well as for law enforcement). Significant concern was voiced by the participants about the unavailability of rapid diagnostic tools. Without rapid analysis, triage becomes a nearly impossible task as little can be done other than immediate decontamination.

The biggest issue facing the team was crowd control and medical response. Consequence management is handled by local law enforcement, while the crisis management is handled by the federal agencies, i.e. the FBI is responsible for evidence handling, but they will not handle triage medical care. Clearly without capability to rapidly analyze the gas, the initial decision will be to just postpone and have people go back to their hotels and then reconvene the next morning.

Recognizing the critical role the media will play in this situation, the JOC will necessarily need to include professionals who will be charged with handling the media response. The Secret Service will immediately remove the President from the scene, while local authorities have the primary responsibility for treating the victims. In particular, the local fire department and EMS are in full control and, without rapid assessment tools, their first response will be to hose off those contaminated and treat them for any symptoms at the scene. Local hospitals will be notified. The team was worried that there is not likely to be enough fire fighters and EMS to handle the response for a mass casualty event. There was great concern about how to keep the people in place, that is, to keep them from either returning to their hotels or home. Obtaining consensus for treatment could be a significant issue, and one not necessarily easily addressed. There was general agreement that people would not be detained as the US is not a police state. While a local state of emergency could be declared, this would take hours. By the time of any declaration, many of those affected will have already left the scene.

Fifteen minutes into the discussion the team was told that a search of the auditorium in the area where the initial odor was detected turns up a tank that is similar in appearance to an oxygen tank used by sufferers of emphysema or other lung disorders. The valve is open and, although the tank is empty, there is a strong acrid odor.

All agreed that at this point in time the FBI would be responsible for gathering forensic samples, including air samples and swipes from inside the convention center. However, air samples and swipes lifted from the building would take at least 48 hours to process. Additionally, there would need to be a determination of whether the gas release was accidental or intentional.

In this scenario, as people were driven out of doors by the initial attack, they were detained in the area around the convention center by law enforcement as well as medical triage. There is a possible threat of a secondary attack on the confined audience with lethal agents from upwind and outside the immediate security area; however, this phase of the scenario ends before this secondary threat can be confirmed. These events raise numerous questions regarding the handling of crowds following a disruption that may be diversionary, as well as concern over whether and how individuals can be quarantined. For example, can you declare martial law? Do you just treat those with symptoms without having a firm diagnosis and what are the ramifications of following this procedure? Finally, how do you handle the risk of secondary exposure to both first responders and the public?

Thirty minutes into this discussion, the local television station announces that it has received a message from a terrorist group claiming responsibility for the attack and stating that plague bacteria (*Yersenia pestis*) was released in the vicinity of the convention center. The FBI is notified, and the television station broadcasts the terrorists' message. Again the CS team is asked to address the following issues:

- ¥ Who will make the decision about whether to continue with the convention?
- ¥ If it is cancelled, will the attendees be allowed to leave the area? Who decides and when?

The CS group generally agreed that the local FBI will now assume that this was an actual attack. Then, because this is now a crisis management situation, the governance would shift to the FBI. There was also discussion of heightened concern over the possibility of a secondary attack now that the people have been driven out of doors. The highway patrol would be on alert to vehicles in the vicinity, and there would be swipes down at the convention center. Threat assessment would be done to determine whether there is a credible threat (and from whom). However, it will take 6 to 12 hours just for the first phase of this assessment -an evaluation of the likelihood that this is a hoax. Additionally, since the gas release is in the front two rows of the convention center, there will be cameras that would have data that would need to be examined for evidence of any suspicious activity.

In the final move of the scenario the abandoned RV is found on the freeway and the valve on the propane tank on the outside is found to be open. There is a second tank inside the RV that is closed and has a label marked SARIN. The media is on hand when this is found and they report the presence of the tank of chemical weapons material. In addition, the local media find and interview an expert who explains the symptoms of Sarin to the public. Within hours the local emergency rooms in the area are overwhelmed with conventioners exhibiting shortness of breath, and runny noses. Again the team is presented with questions:

- ¥ How do you handle the second chemical tank?
- ¥ What do you do about the bio threat? (Inoculate, quarantine, treat?) Will you wait for culture results before administering antidotes?

- ¥ Do you attempt to decontaminate and how?
- ¥ How are media releases handled?
- ¥ How do you handle contacting the conventioners?

There was significant discussion about the need to reassure the public about the risks and counter the media frenzy that has been created. However, in doing this it is critical that the situation be assessed properly and that accurate information is provided. For example, if there is a secondary attack, the first responders will likely be among the first to fall victim. How do you decide whether to use inoculations and how to prioritize the delivery of prophylaxis? Additionally, it will be important to notify the media that Sarin, while highly toxic, is also fast acting. Since there have not been any victims observed, in all likelihood, there has not been an exposure. The JOC will play a key role in disseminating information. Again, however, accurate information is key. A hot line should probably be established, and experts made available to answer questions.

Fifteen minutes into the discussion the team is finally told that the tank in the convention center was found from headspace sampling to contain sulfur dioxide (SO<sub>2</sub>). This information raised the following questions:

- ¥ Who will contact convention attendees?
- ¥ Who will contact the media?
- ¥ Is there an action plan, and who is responsible?

Again, the JOC plays a key role in disseminating information; however, given that the media has been intimately involved, it will be crucial to work closely with them to ensure that the information disseminated is accurate. Additionally, rapid analysis will be key, but it may not be readily available from accredited labs.

Thirty minutes later, using DNA typing, the team is told that the tank on the front of the RV is shown to contain *Yersinia pestis*. What further tests are to be done on the plague material? (Culturing, etc.?) Note, that the residual plague is probably not viable.

Given that there is now a plausible BW threat, the tenor of the discussion changed significantly. There was a sizeable discussion about how to treat the possible exposed victims. How do you decide on who should receive antibiotics? Would people break into pharmacies? Could you force people to take antibiotics if there is a sense that they were exposed? How would you estimate exposure? Can you declare martial law and conduct a mass quarantine? What role does the Federal Emergency Management Agency play? Where are the robust information systems to allow rapid assessment?

There was general agreement that the existing civil defense agreements are not sufficient. Additionally there is general concern that while this might be a hoax, the current assessment tools are not sufficient to allow this assessment to be completed in

time to avoid having to conduct a program of mass prophylaxis. Additionally, given that many of the convention participants are from out of the area, there would have to be agreements between jurisdictions for treatment and dissemination of information.

## **Three Cities Scenario (TCS)**

### **Background**

The Three Cities scenario begins on the day after Thanksgiving during an influenza outbreak in a major Midwestern city (City One). In addition to high flu incidence among the general public of City One, many members of the medical community (most of whom had received flu shots) at three major hospitals have begun to report in sick with flu-like illness. Serology samples from several of the ill medical personnel were taken, but results did not become available for nearly a week. Once available, the results showed that Q Fever, not influenza, was the primary infection agent among the sick medical personnel. Per federal reporting guidelines, the Centers for Disease Control (CDC) were immediately notified. Additional serology testing revealed that many civilian patients with flu-like symptoms had also been exposed to Q Fever.

About ten days after these events, another outbreak of flu-like symptoms among medical personnel is detected in a major southern city (City Two). The CDC alert based on the outbreak in City One led to prompt serologic testing and Q Fever is confirmed. Both the CDC and the FBI are notified.

CNN reported early this morning that two US cities have been attacked by terrorists using biological agents (without naming Q Fever) which induces symptoms that resemble the flu, and that dozens have died. Following the CNN report, clinics and hospitals across the country are overwhelmed by frightened people suffering flu-like symptoms; job and school absenteeism has skyrocketed, and lines are appearing at grocery stores and gas stations.

A third large metropolitan area (City Three, which is relatively near City Two) is also in the midst of a flu outbreak. Only a handful of cases of Q Fever have been identified, and these appear to be associated with travelers who were recently in the other two cities.

### **Scenario Play**

The emergency planning staff in City Three is gathering to develop contingency plans for their metropolitan area to deal both with an actual Q Fever attack and with the public panic caused by the CNN news stories about biological terrorism. For the play of this scenario, the Three Cities group (TCG) was comprised of a team of technology experts, local emergency responders from three US jurisdictions and one international jurisdiction, a physician, and several federal officials. This group was told they represented the emergency planning staff for a large southern metropolitan area (some 3 million people in 13 counties and numerous local jurisdictions).

With this background information, the TCG began its discussion. The participants agreed that the most important requirement was access to information. Since Q Fever is a zoonotic disease, there is a requirement for a strong veterinary input. The TCG requested access to a portable computer as well as the Internet. This importance was emphasized both from the perspective of the medical community and law enforcement participants. The general first reaction of the players was What is Q Fever? This unfamiliarity was particularly evident in the non-medical (e.g., emergency management, law enforcement, etc.) communities, making access to information to fill this knowledge gap important.

The general conclusion was that the diagnosis of Q Fever was discovered quite by accident and not by systematic evaluation. There was general agreement that the initial report from City One obviously helped speed the diagnostic process in City Two. The TCG concluded that the most appropriate technical support to deal with this outbreak would be -- a microscope. Treatment was the next major concern; the antibiotic tetracycline is recommended for treating Q Fever. However, according to the resident medical expert, the medical community nationwide needs education regarding both the appropriate and inappropriate treatments for this and other bacterial and viral agents. For example, use of tetracycline is contra-indicated as a treatment for influenza.

The TCG agreed that the press reports were contributing to public confusion. Though they had access to the Internet, their concern continued over the lack of access to information for addressing specific questions. They felt this lack of information impeded their success in developing a coordinated plan for a sprawling area like City Three. There was great concern that any plan based on incomplete or confusing information would be inadequate to calm the general public and, in fact, could exacerbate panic.

The plan developed by the TCG initially consisted of an information sheet on Q Fever, emphasizing that, in the overwhelming majority of cases, it is not a life-threatening infection. The team's goal was to prevent panic and to ease the overwhelming demands on health care providers.

Following the TCG's initial discussions and development of the information sheet, the TCG was told that the local FBI office reported that some samples taken from buildings near affected hospitals in the first two cities showed Q Fever residuals. The FBI report further stated that the virus was ...probably disseminated into the air in and near medical facilities from a moving vehicle, possibly a large truck... They were also told that the Associated Press reported that anonymous threats of imminent biological attack have been received by news media in at least twelve major US metropolitan areas. The TCG concluded that this new information indicated that the Q Fever virus had been deliberately disseminated near medical facilities in both Cities One and Two.

Ultimately, the TCG concluded that the possibility of terrorism had to be taken seriously, given the threats that have been received in various jurisdictions. However, they were not convinced that their municipal area had actually been attacked. Thus, the group felt they were still dealing primarily with a public health problem. As a consequence, the TCG felt that the greatest need was for a plan to inform people about what Q Fever is, to emphasize that it is generally not a serious problem, and to emphasize that the problem (if any) at this point is only the threat of Q Fever, not something worse. They also concluded that an announcement should provide information about specific clinic locations for screening those taken sick, to ease pressures on local hospital emergency rooms.

Particular targets for this information would be personnel in medical facilities and nearby locations and people who are at risk for developing serious complications should they become infected. The group determined they would need to use the local media (particularly TV) to help with this information dissemination campaign. An important goal of this plan is to reduce anxiety and avoid public hysteria. The TCG did raise the issue of coordination with other cities, but took no action. From the standpoint of the contribution of existing technologies to the TCG's planning, the group regarded the scenario as presenting largely a public health problem. Important issues at this point involved organization and logistics planning, not technological detection, monitoring, and prevention measures. However, the group did discuss the possible exploitation of existing technological devices such as rooftop aerosol collectors to help with detection and mapping of Q Fever virus.

The TCG is told that three days later the public relations campaigns have been effective in reducing public fears. Additionally, to date, the Q Fever attacks have resulted in about two dozen deaths. Threats, claims of responsibility, and so forth have continued to dribble in throughout the country.

On this same day, someone broke into the Fox News web site in City Three and posted a message claiming responsibility for attacks in Cities One and Two, and threatening an attack with anthrax by supporters claiming connection to an ethnic group involved in an international conflict. Similar messages were also delivered to various media in at least a dozen other US cities.

Much of the TCG's discussion following this news centered on whether this anthrax threat could be anything other than a hoax. Hoaxes involving anthrax are common, partly because criminal use of it as a biological agent is extremely difficult.

The TCG discussed many options. The group could inform the public that hoaxes are common and that an actual attack is a very low probability event. They could inquire as to the availability of national assets for detection, but that idea was dismissed because of competing demands from other cities that have received similar threats. The

TCG wondered what to tell authorities to look for. An aerosol truck dispersal system? A crop duster? The TCG also considered additional security at vulnerable facilities, but because no specific targets were identified in the latest threat, the TCG felt unable to define vulnerable facilities. Finally, the TCG concluded that the most immediate problem was responding to public concerns about the anthrax threat rather than actual planning and preparation for countering the threat. The TCG felt it needed a strategy for damage control from a public relations perspective, to allay public fears.

Unlike the situation with the Q Fever threat, the TCG felt there were identifiable issues for law enforcement since hacking into the Fox web site with the stated threat would constitute WMD extortion. Law enforcement authorities could now attempt to track the hacker(s). Threats delivered through other media in other jurisdictions could be tracked using forensics, etc. One of the group members raised the issue of help from federal sources; however, the consensus was that this would not prove terribly useful because federal agencies don't share classified information with local jurisdictions.

At this time the TCG was told that all state governors had received a message from the President's National Security Council (NSC) stating that the Central Intelligence Agency (CIA) deemed the anthrax threat to be credible.

TCG group discussions resumed with a slightly heightened sense of urgency. The TCG did not want to unnecessarily alarm the public about something that is a very low probability occurrence. On the other hand, the TCG didn't want to ignore the threat only to have it materialize. The effects on public confidence of cavalier dismissal of a threat that materialized would probably be worse than the actual consequences. The TCG believed it needed to add experts on anthrax and epidemic management to its ranks. It also felt the need to conduct an inventory of antibiotics available to treat any occurrences of anthrax.

Again, the TCG team focused their efforts on a public information campaign including a noncommittal statement that put recent events into perspective. The statement reminded the public about steps that need to be taken for decontamination in the event of possible exposure to anthrax spores. The TCG group specifically rejected the notion of a vaccination campaign because the risks of inciting panic were not worth the potential benefits of having even some part of the population vaccinated against the very remote possibility of an outbreak.

The TCG also concluded that, in the absence of specific real-time anthrax monitoring technologies, air sampling for the presence of anthrax spores could be accomplished by using existing, relatively low tech, rooftop air quality monitoring devices throughout the metropolitan area. The TCG specifically discussed using in-place Environmental Protection Agency devices as well as those on university campuses, testing small samples of the filter elements for the presence of anthrax spores.



The TCG was informed that, approximately two weeks later, the President held a news conference and revealed publicly the existence of threats of terrorism directed at US citizens both at home and abroad. The President announced that the US would hold the sponsoring foreign government responsible for any attacks against US citizens.

Additionally, the TCG team was given an FBI bulletin reporting that an abandoned liquid oxygen tractor-trailer had been found in City Two. Testing suggested that it had once contained Q Fever virus. Law enforcement officials also discovered that the truck's pressure valve had been altered to allow for controlled leakage of the contents while the truck was in motion. The FBI believes that this truck was the means of dissemination of the Q Fever virus in City Two and, possibly, City One. Attempts to determine who owned and operated the truck are underway.

The TCG planners remain concerned about how to promptly identify a real anthrax attack. There was consensus that an outbreak of pulmonary anthrax in animals would set off alarm bells in the veterinary community. This would be likely to prompt the vet community to inform the CDC. The TCG decided that, for now, it should continue with the public education program and the ad hoc provisions for air sampling. Draconian measures such as stopping all tanker trucks within and/or entering the state on interstates were deemed premature (and, quite possibly, an unconstitutional search and seizure).

In the midst of these deliberations, the TCG was told that a liquid oxygen truck has been hijacked during a delivery of liquid oxygen to a hospital in City Three. The driver was knocked unconscious and his uniform stolen. There was considerable discussion regarding the availability of technological devices to assist in the search for the truck. Was the stolen truck fitted with any kind of tracking device? Could aerial surveillance recognize liquid oxygen being dumped? (The TCG consensus was probably not.) Could satellite imagery help in the search? (Probably not.) Since information on such thefts is collected and disseminated nationwide, the local authorities would have nationwide law enforcement resources available to them if the truck had been driven across state lines. As authorities search for the truck they will have to give appropriate consideration to constitutional protections against unreasonable search and seizure.

The TCG group considered and rejected the idea of making some sort of public announcement about the truck hijacking. There was no hard evidence that the hijacking had anything to do with any of the earlier events. Thus, the group concluded that the appropriate course was to vigorously pursue the investigation of the truck theft and to avoid arousing further public concern by making an announcement that would suggest a linkage of previous events, threats, etc., with the hijacking. The TCG concluded that, if the media made such a connection, they would have to be prepared to deal with the fallout.

At this point, the TCG received a final message informing them that the FBI had arrested seven suspected terrorists this morning and had intercepted a container of *Yersinia pestis* (plague). The container was believed to have passed through Kazakhstan, and the CIA believes that the bacteria may have been provided by sources in Russia. The FBI message says it cannot rule out the possibility that other containers of plague are en route to other destinations in the US. In the TCG this new information caused much concern and discussion, but basically did not change their plan for an emergency response consisting mostly of public information and public confidence building. The public information campaign would now have to focus on informing citizens about the nature of plague. The TCG believed special emphasis should be placed on the difficulty of weaponizing plague due to the amounts needed and the difficulties of dissemination. Plague can also be treated with drugs, but, unlike Q Fever and anthrax, it is highly contagious. Part of the TCG's revised public information campaign would also be targeted toward the medical community to insure that it avoids being caught up in hysteria and remembers that, Everything that coughs isn't plague.

While the TCG planners continued to be mindful of potential future problems and challenges (e.g., this could turn into a massive, nationwide public protection campaign -- including protecting people of certain ethnic descents from their panicked neighbors), for now their focus remained on public education and public confidence building. The TCG viewed as their worst immediate enemy the effects of panic.

## **Findings**

During the first iteration both teams were told that they could deploy any or all technologies currently in the possession of any team member. Despite this generous ground-rule, few current technologies were actually used by either of the teams. From the control group's debriefings of each team following the first iteration, it was clear that few of the currently-available technologies were deemed useful under either scenario. Many participant comments were focused on the unsuitability of many of the technologies on hand. Complaints covered a gamut of failings: too costly ; requires too much training ; doesn't give fast enough answers ; needs three guys in lab coats to keep ready for operation ; too fragile for field use ; too complex for field use in a crisis ; can't trust the results .

After completion of the first iteration of these scenarios, several technology developers provided detailed briefings on their current R&D efforts, specifically focusing on the following areas:

- Capability, including needs assessment
- Size
- Validation/Accreditation
- Cost, initial as well as long term
- Training
- Maintenance requirements
- Investment, including cost, manpower, and training
- Operational issues

Technologies discussed included several different chemical and biological sensors (both wide-area, real-time remote monitoring, and hand-held devices), the use of early warning networks, smart buildings, atmospheric release monitoring and modeling systems, information systems for consequence management, and information systems for epidemiology and rapid diagnosis.

Following these presentations and questions from the participants, teams replayed the two scenarios, with the proviso that teams could use any of the emerging technology options presented (or others they were aware of), provided they met team constraints for ease of use, training and maintenance requirements, cost, investment, etc. Teams were also instructed to consider and prepare to discuss the likelihood that their home jurisdiction would actually buy any of the chosen technologies when available.

The results of the scenario replays were most enlightening. Each team first developed a shopping list of new and existing technologies that they found useful for

preventing and/or responding to different types of WMD threats, regardless of cost or other tradeoff. These included:

Chemical:

- Sensor networks that can detect all known threats
- HAZMAT teams trained with the latest technology
- Personal protection equipment for all first responders
- Hand-held monitors and mobile labs in place and readily deployed
- Stockpile of prophylaxis medications

Conventional Explosives:

- Explosive sniffers
- Electronic counter-measures
- CCTV
- X-ray of packages

Radiological:

- Nest teams and mobile vans
- Portals
- Hand-held monitors

Biological:

- Sensor arrays for ready deployment
- Air and Surface sampling
- Large scale rapid screening techniques
- Epidemiological surveys of areas before an event or on a continual basis
- Hand-held monitors
- Mobile labs
- Information and training for physicians on BW risk, diagnosis, and treatment
- Stockpile of antibiotics

In addition to considering the technologies briefed to players, teams also requested access to other innovative information systems. For example, they requested systems (either through commercial services or as readily available software packages) with the capability to easily map meteorological data and/or overlay plumes, as well as to map outbreak data through a user friendly front end and simple pictorial representation. They identified a need to conduct large scale sampling of the population (both ill and healthy), to have someone to maintain this data, and to make it readily available upon request, as well as to develop rapid techniques for identifying outbreaks. They discussed the possibility of utilizing samples from existing pollution monitoring filters, already widely in use in major metropolitan areas, as a screening device for detection of chemical and/or

biological agents. In addition, participants thought medical information systems would be valuable to all the emergency response communities, for medical treatment, rapid diagnosis, and law enforcement.

Finally, teams raised the problem of false alarms (false positives), whether for law enforcement or health monitoring. False alarms are not tolerated well by the general public, and there was substantial concern about the loss of official credibility due to false alarms. Decisions made based on a false alarm can not only waste precious time, but can lead to additional loss of life.

After identifying all the desirable technology items above both for emergency response and consequence mitigation, the teams were confronted with considering whether their jurisdiction would provide them with these technologies. Most responders were of the opinion that the technologies would not be acquired by their jurisdictions, nor, if purchased, would they be able to properly maintain, and train personnel in the use of them. Their most fundamental constraints dictate that new technologies must be **inexpensive, reliable, and simple.**

In addition to providing a forum to bring these disparate communities together, this workshop also provided a mechanism for sharing information on efforts that are working. For example, the technology community is involved for the first time in the application of consequence management tools for the winter Olympics planning underway in Salt Lake City. This is providing useful feedback to the technology developers as well as a useful tool for the response planning in Salt Lake City. Additionally, the Los Angeles County emergency response community is well aware of technology developments and has reached technology-sharing agreements with several of the government Labs. In addition to providing input to the development community, LA County has organized in a very unique way that was of great interest to the other cities. LA has formed a terrorism early warning group that includes local, state, and federal officials representing law enforcement, fire, medical, health, and emergency management. The other communities present were very interested in this novel approach, and were quite forthcoming in describing this workshop as an excellent opportunity for them to learn from one another.

We had a representative of Scotland Yard participating in this workshop. It was most useful for the first responders from the US cities, as well as for the technology developers, to discuss with him the different approach taken by the UK in planning for a WMD terrorist incident. Based on 30 years of experience in dealing with threats and actual incidents, the UK, rather than assuming a defensive posture (only focusing on responses to events), presumes that a terrorist event is highly likely sometime in the next five years. Thus, major emphasis is placed on planning and intelligence for preventing and mitigating the effect of an event.

## Conclusions

This workshop provided a useful forum for the emergency response communities to share ideas and concepts among themselves, as well as to engage the technology community in discussions. Technologists have been working to develop tools largely in a vacuum, not taking into consideration the special needs of, and constraints on, emergency responders. One key finding is the need for detection technologies that are **inexpensive** (less than ten cents each), **reliable** (rugged and maintenance-free) and **simple** (no training required, red light or green light, or like a home pregnancy test). A second key finding is the need to develop a mechanism for providing access to expertise and tools that may not yet be commercially available (e.g. access to R&D scientists and cutting edge analytic tools). However, these tools need both to be validated and to have clear user manuals explaining their capabilities, limitations, and error rates. Third, physician training and awareness was identified as an easily satisfied need, but one that requires a specific organization or body to develop, offer, and monitor. Fourth, a regular forum should be established to allow these disparate communities to exchange information and ideas for new developments as well as lessons learned. Finally, since most of the relevant technology development funds come from federal sources, the federal government must do a better job of ensuring that the real needs of, and constraints on, emergency response organizations are recognized in the funding and design of new technologies. Failure to do so will only increase the size of the closets required by emergency responders for storing their latest useless toys. Finally, the participants felt that if we could identify, develop and deploy technologies that focus on prevention and early detection, significant cost savings could be achieved relative to strategies focused solely on consequence mitigation and response.